

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

KONNECH, INC.,

Plaintiff,

v.

TRUE THE VOTE, INC., *et al.*,

Defendants.

§
§
§
§
§
§
§
§

Civil Action No. 4:22-cv-03096

DEFENDANTS’ OPPOSED MOTION TO DISSOLVE PRELIMINARY INJUNCTION

Defendants Catherine Engelbrecht, Gregg Phillips, and True the Vote, Inc. petition this Court to dissolve the preliminary injunction issued on October 31, 2022. The Court of Appeals on the recent mandamus petition, *Phillips*, No. 22-20578, 2022 WL 17175826, at *1 (5th Cir. Nov. 22, 2022) (hereafter “*Phillips I*”), ruling on Defendants’ petition for writ of mandamus (titled “Mandamus from the United States District Court for the Southern District of Texas,” hereafter “First Petition”), filed on November 3, 2022, stated “the district court’s TRO was invalid because it disregarded the order of operations imposed by the Federal Rules.” The Fifth Circuit went on to hold that “[i]t necessarily follows that any contempt order premised on violations of the [invalid] TRO was ‘bottomed irrevocably on a mistake of law,’” citing *United States v. Dickinson*, 465 F.2d 496, 514 (5th Cir. 1972). It also necessarily follows that the preliminary injunction, which mirrors the invalid TRO, must be dissolved. In the alternative, Defendants assert that because the preliminary injunction, like the TRO, puts the “cart before the horse,” and amounts to a premature discovery order, the Court on its own may and should dissolve the preliminary injunction.

I. Introduction: Plaintiff and the Court were Confused About Which Computers are at Issue

In *Phillips I*, the Court of Appeals held that the proceedings here failed to identify any “emergency,” or danger of irreparable harm, that would justify a TRO or preliminary injunction. The Court of Appeals could also have premised its finding of a lack of emergency on Plaintiff’s failure to state a CFAA claim with any likelihood of success on the merits. In any event, these are the two primary deficiencies we address here.

The pleadings referring to web pages and podcast transcripts Plaintiff cites to justify the allegation of an emergency CFAA claim are consistent about one thing: the parties are talking about computers, but they’re not talking about the same computer.

Plaintiff, outraged by what it views as defamation, has filed its Complaint, Motion for TRO, and other pleadings alleging imagined violations of the “**Konnech computer**”. We know the Konnech computer has never been breached, because the Konnech computer, Konnech assured visitors to its website, is secure. There is no evidence any Konnech computer has ever been hacked, by anybody, anywhere. The Konnech computer is owned by Konnech. The Konnech computer is physically located in the United States.

Meanwhile, the Chinese Server that *Defendants* are talking about in the same podcasts is not in the U.S. (Defendants aimed to confirm this in the October 27 and 30 show-cause hearings with testimony from the Los Angeles County DA’s Office, among other means). Defendants’ public statements and testimony consistently feature a “server,” as a type of computer is called, located in *China*. This server was *not* secure. This server was *not* owned by Konnech. This server was *easily accessed* by third parties. Defendants consistently averred the server alluded to in the podcasts was in China, as did Plaintiff, *see* Compl. ¶¶ 46-48. *There is no evidence in the record indicating otherwise.*

If the unaccessed Konnech Computer and the Accessed Chinese Server look like two different computers, that's because they are. Plaintiff's invocation of CFAA penalties and fines thus fails for lack of subject matter jurisdiction. The Court must take notice that the same podcast statements made by or attributed to Defendant Gregg Phillips, on which Plaintiff relies, show he has consistently said he viewed data from a computer *in China*.

In Plaintiff's Response to Defendant's Petition for Writ of Mandamus (hereafter, "Response"), Plaintiff offered neither contrary evidence nor even a rebuttal rooted in Defendants' actual statements. Its Response simply appended transcripts from Defendants' podcasts, which confirmed Plaintiff's wholesale reliance on conjectural square brackets and tortured paraphrasing to allege conclusory "access" of a "Konnech computer" in the United States. What claim had Konnech, then, to any likelihood of success?

II. Plaintiff Failed to Establish the District Court's Subject Matter Jurisdiction

"Subject-matter jurisdiction cannot be forfeited or waived and should be considered when fairly in doubt." *Ashcroft v. Iqbal*, 556 U.S. 662, 671 (2009). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008).

Plaintiff here staked its claim to the power of the federal courts (1) on conclusions of law – e.g., that all three Defendants "accessed" a "Konnech computer" – and (2) on implausible representations of Defendants' public statements that would not have survived a motion to dismiss, had Defendants been allowed traditional due process and had the concomitant standard burden of proof been applied and administered. Plaintiff certainly would not have satisfied the even higher standard required for a TRO or a preliminary injunction. The Court should not have credited

Plaintiff's misreading of Defendants' public statements as true. It should have examined the record itself and demanded more evidence-based allegations from Plaintiff.

Almost the entirety of the Complaint and Motion for TRO are taken up by (1) Plaintiff's battery of tendentious, disparaging, and extraneous allegations designed to inflame the reader, and (2) Plaintiff's defamation claims. The kernel of Plaintiff's CFAA claims comes from allegations in Paragraphs 7, 40-42, and 46-48 of the Complaint. Based on these allegations, Plaintiff sought a TRO and, later, preliminary injunction, not on grounds of evidence that any of its U.S.-based computers had been accessed, but by virtue of selected quotes Plaintiff has strung together from Gregg Phillips's podcast statements about a server in China. Strikingly, in Paragraphs 46-48 of the Complaint, Plaintiff *admits* that Phillips was always talking about a server in China:

46. . . . Defendants have falsely accused Konnech of storing sensitive and personal data—including social security numbers, email addresses, phone numbers, and banking information—on 1.8 million U.S. poll workers *on servers in China*, and otherwise running their election logistics application through *Chinese servers*.”

47. And during the September 5, 2022 “Tiger Project” podcast advertised by Defendants, Defendant Phillips falsely claimed that Konnech “left a database open that had the personal identifying information of over a million Americans living *on an open server in China*.”

48. Similarly, on the “Here’s How They’ll Try to Steal the Midterm” podcast mentioned above, Defendant Phillips falsely claimed that Konnech’s election software “apps *were running from China, the database is running in China. It’s on the Chinese internet, meaning the Chinese own it*.”

(emphases added)

So it's inexplicable that, though Phillips never mentioned Konnech in the quoted podcast segments, Konnech, in its Complaint's Paragraphs 40-42, tries to insert itself into a stated CFAA claim via two misleading methods: (1) Konnech ends Phillips's quoted content and then inserts the word “Konnech” in place of the Chinese server or data Phillips is talking about, and (2) Konnech keeps the quotation marks but inserts “[Konnech]” in square brackets meant to signify to a reasonable reader that “Konnech” is plausibly what Phillips was speaking about. We can see

the latter misleading method at work in Paragraph 40, which refers to the Prophets and Patriots podcast:

Indeed, Defendant Phillips admitted on that podcast¹ that “[w]e took [Konnech’s data] directly” and that Defendant True the Vote plans to publicly “release all of [Konnech’s] data” through “drops” to subscribers of Defendants’ website.

What Phillips said was “We took *it* directly” -- and it’s not at all clear from the context what he meant by “it” or even “took” -- and, much later, “we’re gonna release *all of our research*” (i.e., research on the existence of breaches in elections systems) (emphases added). If one listens to the podcast from which Plaintiff cherry-picks, at 39:50, it is clear Phillips is talking about a server in China:

. . . But what if your data was all being filtered *through China*? . . .

. . . We took it directly. That was on a Friday after Friday. Now, my guys invited me to Dallas on a Friday night. We went, met at a hotel room, towels under the doors. It was pretty weird. I mean, it was like some kind of a James Bond kind of thing or some sort of weirdness like that. And they proceeded to show me everything. They showed me the database, they showed me where it lived. *It lives on the main unicorn* [sic – Unicom] *backbone in China, which is the main Internet in China.*

(emphases added). In Paragraph 41, Plaintiff misrepresents the contents of another podcast:

41. Defendant Phillips repeated these claims on an August 30, 2022 podcast titled, “Here’s How They’ll Try to Steal the Midterms,”² where Phillips described, once again, traveling to Dallas, Texas to meet his so-called “analysts,” where they “plugged one of their computers into the television” and began “scrolling through millions and millions of records about Americans,” *all of which he claims to have obtained by gaining unauthorized access to Konnech’s protected computers.* Defendant Phillips also described how he “immediately drove down to Houston” and got Defendant Engelbrecht “to come over and meet [him]” that next morning, where they came up with a plan to file a complaint with the FBI *and turn over the data they stole.* (emphases added)

¹ “Prophets and Patriots”: <https://rumble.com/v1h1pj9-rumble-only-prophets-and-patriots-episode-20-with-gregg-phillips-and-steve-.html>

² See <https://rumble.com/v1hz1jr-heres-how-theyll-try-to-steal-the-midterms-gregg-phillips-interview.html>.

To patch together Paragraph 41, Plaintiff must forage across the transcript, piecing together language out of context to suit its narrative. The “plugged one of their computers” language comes from the 35:29 mark. But Phillips’ statement there plainly says the accessed server was in China, and at 34:54 he even explains how he knew it was in China:

[The website Binary Edge] tells you where it lives, where does the server live, and you could actually track it down and you track it down to China. On the main unicorn [sic; Unicom] backbone in China, it was almost impossible for me to believe.

For the language about “scrolling through millions and millions of records,” Plaintiff must leap to a different part of the transcript, at 36:57. But once again, the full quote (from 36:21 to 37:14) even of this excerpt shows Phillips was clear about the server being in China, and “Konnech’s computers” are nowhere in sight:

[T]he other thing that your fearless listeners need to understand is that *by Chinese law, if something comes onto the Chinese backbone, in other words, it's in the Chinese Internet*, that means the CCP owns it. What I'm telling you is that that night in mid-January of 2021, I personally witnessed the scrolling through of millions and millions of records about Americans. We later found out that that was attached directly to the [Chinese] social scoring system . . .

(emphases added)

Plaintiff employs a similarly misleading device in Paragraph 42 of its Complaint, where, like an unwelcome guest at a party, Plaintiff inserts itself into conversations that did not involve it:

42. Likewise, on a September 2, 2022 podcast hosted by Defendant Phillips called “Patriot Games” . . . Defendant Engelbrecht . . . confessed to how Defendants conspired to *unlawfully access Konnech’s protected computers*, and how she and True the Vote “pulled in [Defendant Phillip’s] team, and asked them to take a deeper dive” *around the security of Konnech’s software*. Defendant Phillips told The Pit attendees that they accessed *Konnech’s* alleged *Chinese server* by using a password after finding vulnerabilities in the server.

(emphases added). The Court would hear in the audio of the actual podcast no such “confession” of unlawful access. But even if Defendant Engelbrecht, who was not alleged to be present, could

have somehow “confessed” to accessing a server, *Plaintiff itself* makes clear that the server each Defendant was referring to was an insecure “Chinese server”, which is fatal to Plaintiff’s allegation anyone gained access to one of its secure, U.S.-based computers.

It has become clear that Plaintiff does not want to acknowledge ownership of the only server (the Chinese Server) for which it offers such weak “evidence” of access, by at most *one* Defendant. Plaintiff’s reluctance could be due to the fact that Konnech really did not own the server – though it still very much wants entrée to federal jurisdiction and CFAA penalties. Or Konnech did own the server in China, but knows its customers, to say nothing of regulators, would be alarmed if it said so. Konnech has compromised by arguing that when Defendants clearly speak of an insecure Chinese server that Konnech does not claim to own, they are somehow referring to an unidentified U.S. server that Konnech does own. This misshapen compromise fails to state a claim under the CFAA and certainly fails to meet the even higher burden of showing a likelihood of success on the merits or a danger of irreparable harm.

III. Where the Parties’ Publicly Available Statements Agree There’s No Evidence of Access of Konnech’s Computers, Plaintiff Failed to Show Either Likelihood of Success on the Merits or Imminent Harm

A. Plaintiff Failed to State a Claim Under the CFAA.

The first problem with Plaintiff’s strained claim of a violation of the CFAA is that *even assuming Plaintiff had claimed Defendants access of a computer owned by Konnech*, Plaintiff’s Complaint remains vague about stating which provision of the CFAA the Defendants would have violated. This alone should be fatal to subject matter jurisdiction, let alone to any claim of likelihood of success on the merits such as would support a preliminary injunction.

Plaintiff did not appear to have in mind any particular section of the CFAA, including but not limited to Section 1030(a)(1)³, Sections 1030(a)(2)(A) or (B)⁴, Section 1030(a)(3)⁵, Section 1030(a)(5)⁶, Section 1030(a)(6)⁷, or Section 1030(a)(7)⁸. One might speculate that Plaintiff intended to plead a cause of action under Section 1030(a)(2)(C), which relates to “intentional” access that acquires “information from any protected computer”, but whether Defendant Phillips, the only person in the room during any arguable “access”, did so “intentionally” to a computer *owned by Konnech* is a question of fact and law that neither Plaintiff nor the Court addressed.

Plaintiff’s Complaint, in Paragraphs 85 and 99, mentions the \$5,000.00 threshold of Section 1030(a)(4), suggesting that perhaps it intended to claim a violation of that section, which applies to whoever “knowingly *and with intent to defraud*, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.” (emphasis added). But Plaintiff failed to plead any “intent to defraud” on Defendants’

³ Section 1030(a)(1) relates to access that acquired “information that has been determined by the United States Government pursuant to an Executive order or statute to require protection.”

⁴ These subsections relate to one who “intentionally accesses a computer without authorization or exceeds authorized access” and “obtains” either “(A) information contained in a financial record of a financial institution, or of a card issuer . . . , or . . . in a file of a consumer reporting agency on a consumer” or “(B) information from any department or agency of the United States.”

⁵ This section relates to a “nonpublic computer of a department or agency of the United States.”

⁶ This section refers to “transmission of a program, information, code, or command” that damages a computer, such as malware.

⁷ Section 1030(a)(6) applies to whoever “knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if-- (A) such trafficking affects interstate or foreign commerce.”

⁸ This section requires an “intent to extort.”

part, and even if it had, such a pleading would have demanded a fact-based inquiry that would have required discovery or testimony in the ordinary course of a civil lawsuit. In short, it is impossible to conclude that Plaintiff even stated a claim under the CFAA, let alone that it met the higher standards necessary for a preliminary injunction and TRO.

A. Plaintiff's Claims of "Access" Implicated Novel Legal Conclusions Not Yet Addressed.

Plaintiff's allegations include the observation that Defendants stated the Chinese Server was "unsecured" and "was left with default password on [the] database...." Compl. ¶ 24 (screenshot); *see also* Plaintiff-Respondent's Response to the Petition for Writ of Mandamus at 5, 101, 133, 136, 167, 180, 214. But whether such access is truly "without authorization" or "exceeds" what is authorized is a complex legal and factual question that the Court here did not address. Moreover, whether a party can be held to access "without authorization" a computer that auto-populates with its own password, in some factually undeveloped fashion,⁹ is a novel question of law glossed over by Plaintiff. Plaintiff's claim is not only factually problematic but implicates complex legal arguments. In *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), the Ninth Circuit engaged in a lengthy analysis of the statutory language, legislative history¹⁰, the Supreme Court's opinion in *Van Buren v. United States*, __ U.S. ___, 141 S. Ct. 1648 (2021), and

⁹ How exactly the computer did this is not clear from the record, which should also be fatal to any preliminary injunction that fails to explain it.

¹⁰ For example, the Court of Appeals observed that the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, contained language nearly identical to the CFAA provision at issue, and noted that "[t]he similarity of language in [the SCA and the CFAA] is a strong indication that [they] should be interpreted *pari passu*." *hiQ Labs*, 31 F.4th at 1200 (citing *Northcross v. Bd. of Educ. of Memphis City Schs.*, 412 U.S. 427, 428, 93 S.Ct. 2201, 37 L.Ed.2d 48 (1973)). The Court cited the House Committee on the Judiciary, which stated, of section 2701, that "[a] person may reasonably conclude that a communication is readily accessible to the general public if the ... means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." *See* H.R. Rep. No. 99-647, at 62 (1986). Whether the Chinese Server's means of access was "widely known" is a question of fact yet to be decided, and the record is still incomplete on whether the person who did "access" the Chinese Server encountered any indicia of privacy.

the plain meanings of the terms employed to find that the party accused of access there, hiQ Labs, had “raised a serious question” of law as to whether, “where access is open to the general public,” as arguably was the case here, “the CFAA ‘without authorization’ concept is inapplicable.” *hiQ Labs*, 31 F.4th at 1195.

In this case, Plaintiff acknowledges that the accessed server in China featured a pre-loaded password that did not even require anyone to type in a password to access the server. Plaintiff has argued that use of the password – and whether “use” is even the correct concept is unknowable without testimony from the person who actually accessed the Chinese server – was “unauthorized,” but Plaintiff can offer no legal support for this conclusion. The Court here seems to have assumed that such access of the Chinese server was “unauthorized access”, without considering whether the existence of a default password on the server rendered access the equivalent of, say, password sharing among friends and family, which would inadvertently “make criminals of large groups of people who would have little reason to suspect they are committing a federal crime.” *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012). There was also no discussion in the prior pleadings considering whether a plaintiff that had not claimed ownership of a Chinese server to which defendants allegedly “admitted” access had any standing to bring a claim of access of that computer in the first place.

B. Plaintiff’s Claims Could Not Survive the Lower Standard of a Motion to Dismiss.

The Supreme Court has warned that “the tenet that a court must accept as true [on a motion to dismiss] all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice. *Ashcroft*, 556 U.S. at 678–79 (2009). Here, Plaintiff’s claims of “access” are both

(1) conclusory in nature – as even a cursory examination of its cited statements confirms – and (2) conclusions of law masquerading as factual allegations.

The second major problem with Plaintiff’s claims of “access” under *Ashcroft* is that “only a complaint that states a plausible claim for relief survives a motion to dismiss. Determining whether a complaint states a *plausible* claim for relief will . . . be a context-specific task that *requires the reviewing court to draw on its judicial experience and common sense.*” *Ashcroft*, 556 U.S. at 678–79, (emphasis added; citations omitted). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft*, 556 U.S. at 678 (2009). “Nor do we accept conclusory allegations [or] unwarranted deductions.” *Southland Sec. Corp. v. INSpire Ins. Sols., Inc.*, 365 F.3d 353, 361 (5th Cir. 2004). As we have shown above and show further below, Plaintiff’s patchwork argument of literary interpretation in place of factual allegations has never been plausible enough to survive the lower standard of a motion to dismiss, let alone justify a preliminary injunction.

D. Konnech Confirmed No One Accessed Its U.S.-Based Computers.

Since the CFAA’s enactment, proper claims of computer access have been founded on a plaintiff’s specific allegations that a computer the plaintiff owned, bearing a unique and identifiable IP address, was accessed by a computer operated by a defendant, which bears a different, unique identifiable IP address.¹¹ Here, Plaintiff has never made the necessary allegations

¹¹ For example, in *Hovanec v. Miller*, 2019 WL 2774338 (W.D.Tex. 2019), the district court engaged in a lengthy analysis of whether a person using an email address on a device with IP address 108.65.34.232, running on a Mac operating system and AT&T Uverse internet account, could be the same person using a different email address at the same IP address. This is how courts identify computers, and proper defendants. *See Live Face on Web, LLC v. Tweople, Inc.*, No. 6:14-CV-44-ORL-22TBS, 2014 WL 12611359, at *1 (M.D. Fla. Sept. 29, 2014) (noting counterclaim plaintiff could “competently” make allegation of computer access “because it was able to track and record [defendant’s] IP address when [defendant] accessed video files stored on [plaintiff’s] server”); *CoStar Realty Info., Inc. v. Field*, 737 F. Supp. 2d 496, 506 (D. Md. 2010) (noting plaintiffs had “offered sufficient evidence that at least raises a

regarding either party's computers, even after Defendants identified, in their First Petition, the specific IP address of the Chinese server, whose access Defendant Phillips did not witness but surmised after the fact.

Indeed, Paragraphs 25 and 50 of Plaintiff's Complaint made clear that all of *Konnech's* "U.S. customer data is secured and stored exclusively on protected computers *located within the United States.*" (emphasis added). In Defendants' Opposition to Plaintiff's Motion for Preliminary Injunction, filed September 12, 2022, Defendants showed the Court that Plaintiff had made even more comprehensive statements¹² that should have called into serious question Plaintiff's argument that Defendants ever "accessed" "Konnech computers":

reasonable inference that IP addresses assigned to" defendant's computers had accessed plaintiff's database); *Tharpe v. Lawidjaja*, 8 F. Supp. 3d 743, 761–62 (W.D. Va. 2014) (discussing IP addresses of plaintiff and defendant and noting defendant had provided "an IP address for this alleged 'third computer,' but provide[d] only his bald allegation to link it to Plaintiff"); *Hately v. Torrenzano*, No. 1116CV01143GBLMSN, 2017 WL 2274326, at *2 (E.D. Va. May 23, 2017) (noting that Comcast records showed a computer with an identifiable IP address, belonging to defendant, had accessed plaintiff's Google account); *Francis v. API Tech. Servs., LLC*, No. 4:13-CV-627, 2014 WL 11462449, at *1 (E.D. Tex. Sept. 11, 2014) (discussing allegations of "hacking" IP address of plaintiff's home computer); *Vine Oil & Gas LP v. Indigo Mins., LLC*, No. 4:19-CV-00346, 2019 WL 4140842, at *2 (E.D. Tex. Aug. 30, 2019) (noting "hundreds" of different IP addresses were alleged to have accessed the plaintiff's database); *Vest Safety Med. Servs., LLC v. Arbor Env't, LLC*, No. CV H-20-0812, 2020 WL 4003642, at *1 (S.D. Tex. July 15, 2020) ("Vest alleges that it examined its website's IP address logs and discovered that Defendants had accessed the website"); *Pixsys Techs., Inc. v. Agemni, L.L.C.*, No. 2:13-CV-1929-SLB, 2013 WL 5739027, at *3 (N.D. Ala. Oct. 22, 2013) (noting IP addresses belonging to defendant had accessed plaintiff's computer); *D&J Optical, Inc. v. Wallace*, No. 1:14CV658-MHT, 2015 WL 1474146, at *3 (M.D. Ala. Mar. 31, 2015) (pointing out that plaintiff's identified "server was remotely accessed from an IP address assigned to" defendant); *Earthcam, Inc. v. Oxblue Corp.*, No. 1:11-CV-02278-WSD, 2012 WL 12836518, at *2 (N.D. Ga. Mar. 26, 2012) (tracking defendant's use of IP addresses to access plaintiff's computer).

¹² Plaintiff's September 10, 2022 statement was accessed before Plaintiff's removal of it at: https://www.konnech.com/images/THE_TRUTH_ABOUT_KONNECH_web_version_09102022.pdf. Plaintiff's admissions are currently preserved, among other places, by the Wayback Machine's Web Archive at https://web.archive.org/web/20220920173106/https://www.konnech.com/images/THE_TRUTH_ABOUT_KONNECH_web_version_09102022.pdf and the Fairfax (Va.) GOP website at <https://fairfaxgop-quickfix1.netdna-ssl.com/wp-content/uploads/2022/10/KONNECH-WEBCACHE-STATEMENT.pdf>.

Accusation: True the Vote claims to have downloaded personal data on 1.8 million U.S. poll workers early in 2021 from an unsecured Konnech server in Wuhan, China.

Truth: Konnech thoroughly investigated True the Vote's claims and found no evidence whatsoever of any breach of our systems or Konnech data anywhere in the world.

Konnech has never stored customer data on servers in China. Konnech stores all customer data exclusively in its country of origin. This means that data belonging to Konnech's U.S. customers is stored on secure servers within the United States. It never leaves the U.S.

In this document¹³ we can see Plaintiff's crystalline clarity, after having "thoroughly investigated" Defendants' podcast statements, that it has failed to state a claim of computer access, a likelihood of success in showing the same, or any irreparable harm to its systems at all:


- Konnech "found no evidence whatsoever of any breach of our systems or Konnech data *anywhere in the world*" (emphasis added)
- "Konnech *has never stored customer data on servers in China.*" (emphasis added)
- "Konnech stores all customer data exclusively in its country of origin."
- "This means that data belonging to Konnech's U.S. customers is stored on secure servers within the United States. It never leaves the U.S." (emphasis in original)

Plaintiff could not have made it any plainer that it lacks any evidence of "access" to its computers, that it has no computers in China – the only place Defendants have talked about servers being – and that the personally sensitive U.S. poll worker data Plaintiff seeks to complain about has never been stored by Konnech outside the U.S., "its country of origin". Moreover, Plaintiff has an affirmative duty to disclose any access of its computers to affected parties, such as its customers,

¹³ Indeed, Plaintiff here so successfully made the case for the lack of any "access" of its computers under the CFAA, and therefore the lack of any federal jurisdiction under that act, that Plaintiff scrubbed the content from its website soon after putting it up, on September 10, 2022 -- two days before filling its Complaint and motion for TRO.

and it has not done so, confirming the absence of proof of any access of Plaintiff's computers by Defendants or anyone else.

Plaintiff argued, in its Response to Defendant's First Petition, that Defendants claim that "because Plaintiff found no breach of its system after conducting an internal investigation—as described in a document entitled 'The Truth About Konnech'—that Plaintiff's computers were not hacked. However, the fact that Plaintiff could not find a breach doesn't mean it didn't happen." Setting aside the fact that Konnech's admissions were damaging enough to its argument to be scrubbed from its website within days, Plaintiff appears to agree that the existence of a breach is, at best, a debatable matter – one that requires proper factual development and expert testimony, as well as a conclusion of law forthcoming only after full briefing. But Plaintiff did not offer factual evidence or expert testimony, and the Court made no reasoned conclusions of law tied to those facts.

Thus, the parties *agree* there is no evidence Defendants ever accessed Konnech's computers. This case of first impression thus features the unusual CFAA plaintiff who insists to the world that it has thoroughly audited its systems and can confirm it has never been hacked, while arguing to the courts that its obvious misrepresentations of Defendants' public statements about servers in China somehow prove that Plaintiff's U.S.-based computers *were*  hacked.

E. Plaintiff Has Failed to Claim the Only "Accessed" Computer Was Its Own.

In lieu of its 273-page Response to the First Petition, Plaintiff had at hand a short, simple means to state a claim of CFAA "access" here: Plaintiff could have claimed ownership of the IP address Defendants provided, in their First Petition, for the accessed server based in China. Plaintiff did not.

Instead, Plaintiff fell back on its shamelessly misleading use of square brackets to suggest that when Defendants said “computer”, in statements scattered across the Internet, they can only have meant “[Konnech] computer,” and that when Defendants said “the data” or “it” they were, by some means inaudible to the average listener, talking about “[Konnech] data.”¹⁴

F. Defendants’ Unrebutted Testimony Also Made Clear Their Public Statements Showed No “Access” to a “Konnech Computer”.

Defendants have been consistent in maintaining both publicly and in court that they never “accessed” a “Konnech computer”. In what remains the only testimony on the record, Defendants consistently made clear that they did not hack into or take data from the only server they have ever talked about, an *insecure* server based in *China*. See First Petition (discussing the distinction between Chinese Server Data, a portion of which Defendant Phillips saw after its access, and the very different Election Breach Information they wished to publicize). Indeed, in the only actual evidence presented to the Court by either party, Defendants’ unrebutted testimony at the October 30 show-cause hearing made clear only a server in China had been “accessed,” and not by Defendants. Thus, the parties agree that there is no evidence or even a plausible allegation of access of Plaintiff’s computers by Defendants.

Taking judicial notice of the parties’ public statements, the Court may conclude that Plaintiff’s claims of “access” were based solely on demonstrably “conclusory allegations” and “unwarranted deductions.” Had it been considering a motion to dismiss, the Court could have rejected, as lacking “facial plausibility”, Plaintiff’s plainly flawed conclusion of fact and law: that

¹⁴ For example, at page 7 of the Response, Konnech starts by quoting from Defendant Phillips’ podcast about going into the Dallas hotel room, but then Konnech is obliged to drop the quotation marks as it makes up a not-even-paraphrased allegation that Phillips “proceeded to hack into Plaintiff’s server.” The next sentence exemplifies Plaintiff’s misleading insertion of square brackets ([]) to insert Konnech into its narrative, when no such identification occurred in the original: “Indeed, Phillips admitted on that podcast that he and his team “took [Plaintiff’s data] directly.” In the very next paragraph, the misrepresentations continue, as Plaintiff claims Defendants’ statements prove they “began looking at [Plaintiff’s] data on a server [Defendants] claimed they hacked into.” *Id.*

Defendants, by “admitting” to accessing a computer in China, thereby “admitted” to accessing a computer of Konnech’s in the U.S. The Court could not possibly have gone on to draw “the reasonable inference” that Defendants were liable – and that it had jurisdiction.

The Court could have readily consulted the podcasts offered as the sole basis for federal jurisdiction, as part of the documents incorporated into the complaint by reference or documents integral to the claim, as well as items subject to judicial notice and matters of public record. *See Funk v. Stryker Corp.*, 631 F.3d 777, 783 (5th Cir. 2011); *Agrilectric Power Partners, Ltd. v. Gen. Elec. Co.*, 20 F.3d 663, 664-65 (5th Cir. 1994). If a district court wishes to allow quotations from public transcripts to form the basis of emergency *ex parte* hearings, the Court must satisfy due process by making a reasonable independent inquiry as to whether Plaintiff’s representations of Defendants’ statements amount to conclusory and unwarranted inferences or even, as here, outright misrepresentations.

The simplest route the Court could have taken here, before issuing injunctions, would have been to take judicial notice of Konnech’s own public statements, or to require Konnech to specify the IP address of its allegedly accessed computer. Better yet, the Court could have subjected a Plaintiff witness to the same cross-examination it conducted with Defendants. This should have been done before the Court assumed Plaintiff had stated a claim, that its *unidentified* computers or data were somehow experiencing irreparable harm, or that its imaginary claim of access had any likelihood of success on the merits, and before the Court allowed *ex parte* hearings, early discovery of Defendants, and a contempt order without any testimony at all from Plaintiff.

IV. Plaintiff Failed to Show Imminent Harm to Any Computer, While Defendants Have Already Been Gravely Harmed by Its Implausible Claims.

Plaintiff’s Complaint and Motion for TRO are breathless in their allegations that Plaintiff required urgent, even *ex parte*, relief for some unidentified U.S.-based computer, lest Defendants

seek to harm that unidentified computer or disclose data from it. But where Plaintiff's sole allegation of computer access was based not on evidence but a circuitous argument that when Defendants spoke about a computer in China, not Konnech's, they were somehow identifying a U.S.-based computer that Plaintiff says has never been accessed, the Court cannot have found any likelihood of imminent harm to a "Konnech computer".

At the same time, the individual Defendants, Engelbrecht and Phillips, have already been harmed by the TRO and injunction below. They were subjected to injunctions that were a physical impossibility with which to comply, together with incalculable cost and stress. They were held in contempt and confined in jail for a week under an invalid order of contempt, causing immeasurable damage to their reputations. The balance of harms here thus tilts in favor of Defendants, and the harms are no longer even speculative. The harm to Defendants is real and has already been visited upon them.

V. Undoing the Violation of Due Process Below

Convinced by Plaintiff's misrepresentations of Defendants' public statements, the Court enjoined Defendants to do or refrain from doing about a dozen things that were either pointless or physical impossibilities:

Defendants Were Enjoined ...	Injunction Should Be Dissolved Because...
(i) from accessing or attempting to access Konnech's protected computers	<p>Defendants can of course agree not to do these things. But Plaintiff has provided neither evidence nor allegation that Defendants accessed, or even said they accessed, a computer alleged to belong to Konnech.</p> <p>Rather, unrebutted evidence shows that one Defendant (Phillips) saw data from a server, <i>located in China, after</i> it was accessed, which server Konnech denies owning, and unrebutted evidence from Plaintiff confirms no one accessed its computers.</p>

(ii) to return to Konnech all property and data obtained from Konnech's protected computers, whether original, duplicated, computerized, handwritten, or any other form whatsoever	Unrebutted testimony: no access, no data.
(iii) from using, disclosing, or exploiting the property and data downloaded from Konnech's protected computers	See above item (ii).
(iv) to preserve, and not to delete, destroy, conceal or otherwise alter, any files or other data obtained from Konnech's protected computers	See above.
(v) to identify each individual and/or organization involved in accessing Konnech's protected computers	Plaintiff has provided no evidence whatsoever that Defendants were "involved" in "accessing" any computer alleged to belong to Konnech – rather, unrebutted evidence shows one Defendant saw data from a server, <i>located in China, after</i> it was accessed, which server Konnech denies owning.
(vi) to confidentially disclose to Konnech how, when, and by whom Konnech's protected computers were accessed	See above response to (v).
(vii) to identify all persons and/or entities, in Defendants' knowledge, who have had possession, custody or control of any information or data from Konnech's protected computers	Defendants have identified all persons they were aware had possession of data from the server located in China, but have no information on data taken from a computer alleged to have been owned by Konnech.

Conclusion

The plain language of the TRO that ultimately led to the finding of contempt ordered Defendants, in pertinent part, to "identify each individual involved in accessing ***Konnech's protected computers***" (item v) (and, redundantly, to "disclose" "by whom", item (vi)). But there is no credible allegation in this case that anyone "accessed" a "*Konnech computer*", or even one in the United States. In fact, the parties agree Defendants did not "access" a "Konnech computer". Plaintiff has presented no plausible allegations for, and dispositive evidence against, any CFAA violation.

The TRO and preliminary injunction were thus based on (1) a flawed Complaint and other pleadings and representations that improperly alleged computer access, along with (2) a judicial process that did (a) not allow Defendants to take testimony from Plaintiff or (b) make the barest independent investigation into Defendants' statements, on podcasts, that Plaintiff misrepresented as "admitting" "access" to a "Konnech computer" in the United States.

WHEREFORE, the preliminary injunction should be dissolved (though Defendants can readily agree to abide by the superfluous injunctions of romanettes (i) through (iv)), and the Court should review whether it has subject matter jurisdiction in the first instance.

Respectfully submitted,

GREGOR | WYNNE | ARNEY, PLLC

By: /s/ Michael J. Wynne

Michael J. Wynne

Attorney at Law
Texas State Bar No. 00785289
SDTX No. 0018569
909 Fannin Street, Suite 3800
Houston, TX 77010
Telephone: (281) 450-7403
mwynne@gwafirm.com

Cameron Powell, Esq.
Attorney at Law
DC Bar No. 00459020
Telephone: (503) 502-5030
cpowell@gwafirm.com

James L. Turner
Of Counsel
Texas State Bar No. 20316950
Telephone: (713) 305-5457
jturner@gwafirm.com

COUNSEL FOR DEFENDANTS

Certificate of Conference

I hereby certify that I have communicated with lead counsel for Plaintiff and that Plaintiff is opposed to the motion.

By: /s/ Michael J. Wynne
Michael J. Wynne

Certificate of Service

I hereby certify that a true and correct copy of the foregoing was served by CM/ECF e-service on November 30, 2022, on the following counsel of record:

Constantine Z. Pamphilis
Kasowitz Benson Torres LLP
Wedge International Tower
1415 Louisiana, Suite 2100
Houston, Texas 77002
dpamphilis@kasowitz.com

ATTORNEYS FOR PLAINTIFF

By: /s/ Michael J. Wynne
Michael J. Wynne